



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,934	06/29/2001	David C. Hanley	10014503-1	9392

7590 06/30/2005
HEWLETT-PACKARD COMPNAY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DARROW, JUSTIN T	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/895,934

Applicant(s)

HANLEY ET AL.

Examiner

Justin T. Darrow

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-6 and 9-14 is/are rejected.
- 7) ☒ Claim(s) 7 and 8 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 June 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____ | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

1. Claims 1-14 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 2-5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 2 recites the limitation "the RAM" in line 2. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "RAM" in line 2 and replacing with --first memory element--.

4. Claims 10-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 10 recites the limitation "the RAM" in lines 10, 11, 13, and 14. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "RAM" in lines 10, 11, 13, and 14 and replacing with --first memory element--.

5. Claims 11-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2132

Claim 11 recites the limitation "the RAM" in line 2. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "RAM" in line 2 and replacing with --first memory element--.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-3, 6, and 9-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Rager et al., U.S. Patent No. 5,363,447 A.

As per claim 1, Rager et al. illustrates:

a computer-implemented method for managing sensitive data in a terminal (see column 1, lines 13-16; fixed transmitters for secure information; see column 2, lines 55-57; figure 1, item 101; such as secure transmission device) having

a first memory element (see column 2, lines 62-63; figure 1, item 102; a first volatile memory (RAM)),

a processor having a register (see column 2, lines 66-67; an encryption device containing a second volatile memory (RAM))),

Art Unit: 2132

a security circuit (see column 4, lines 40-43; figure 1, items 101 and 106; a tamper detection circuit), and

a power supply circuit arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source (see column 4, lines 37-40; figure 1, item 101 and 105; a variable power supply powering down the secure transmission device while a constant voltage supply is providing a constant voltage to the encryption device), comprising:

storing sensitive data in the first memory element (see column 4, lines 56-57; figure 1, item 102; storing encryption code and a key in the first volatile memory);

upon loss of power from the first source (see column 4, lines 31-40; figure 1, item 101; powering down the secure transmission device),

switching to power from the second source (see column 4, lines 37-40; figure 1, item 105; while providing a constant voltage to the encryption device), copying the sensitive data from the first memory element to the register (see column 4, lines 31-34; figure 1, items 102 and 106; storing the decrypted encryption code and key from the first volatile memory into the second volatile memory), and

erasing the sensitive data from the first memory element (see column 4, lines 34-36; figure 1, item 102; erasing the decrypted encryption code and keys stored in the first volatile memory); and

upon detecting an attack on the terminal (see column 4, lines 44-45; if the tamper detection circuit activates the reset from detecting tampering),

Art Unit: 2132

erasing the sensitive data from the first memory element (see column 4, lines 34-36; figure 1, item 102; erasing the decrypted encryption code and keys stored in the first volatile memory) and the register (see column 4, lines 44-46; figure 1, item 106; the reset line activated by the tamper detection circuit will erase the second volatile memory in the encryption device).

As per claim 2, Rager et al. further discusses:

upon reapplication of power from the first source (see column 6, line 15; figure 3, step 300; upon power up),

copying the sensitive data from the register to the RAM (see column 6, lines 54-55; figure 3, step 306; storing recaptured encryption code and the recaptured key in the first volatile memory from the second volatile memory in the encryption device).

As per claim 3, Rager et al. then specifies:

that the sensitive data includes a general encryption key (see column 6, lines 54-55; figure 3, step 306; storing the recaptured key in the first volatile memory from the second volatile memory in the encryption device).

As per claim 6, Rager et al. also shows:

that the sensitive data includes a general encryption key (see column 4, lines 13-16; figure 1, item 102; the first volatile memory, which may comprise RAM, is used to store the decrypted keys only while the secure transmission device is powered up; see column 4, lines 56-57; storing a key in the first volatile memory).

As per claim 9, Rager et al. depicts:

an apparatus for managing sensitive data in a terminal (see column 1, lines 13-16; fixed transmitters for secure information; see column 2, lines 55-57; figure 1, item 101; such as secure transmission device) having

a first memory element (see column 2, lines 62-63; figure 1, item 102; a first volatile memory (RAM)),

a processor having a register (see column 2, lines 66-67; an encryption device containing a second volatile memory (RAM))),

a security circuit (see column 4, lines 40-43; figure 1, items 101 and 106; a tamper detection circuit), and

a power supply circuit arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source (see column 4, lines 37-40; figure 1, item 101 and 105; a variable power supply powering down the secure transmission device while a constant voltage supply is providing a constant voltage to the encryption device), comprising:

means for storing sensitive data in the first memory element (see column 4, lines 56-57; figure 1, item 102; storing encryption code and a key in the first volatile memory);

means, responsive to a loss of power from the first source (see column 4, lines 31-40; figure 1, item 101; powering down the secure transmission device),

for switching to power from the second source (see column 4, lines 37-40; figure 1, item 105; while providing a constant voltage to the encryption device), copying the sensitive data

Art Unit: 2132

from the first memory element to the register (see column 4, lines 31-34; figure 1, items 102 and 106; storing the decrypted encryption code and key from the first volatile memory into the second volatile memory), and

erasing the sensitive data from the first memory element (see column 4, lines 34-36; figure 1, item 102; erasing the decrypted encryption code and keys stored in the first volatile memory); and

means for detecting an attack on the terminal (see column 4, lines 44-45; the tamper detection circuit activates the reset from detecting tampering),

means for erasing the sensitive data from the first memory element (see column 4, lines 34-36; figure 1, item 102; erasing the decrypted encryption code and keys stored in the first volatile memory) and the register in response to an attack on the terminal (see column 4, lines 44-46; figure 1, item 106; the reset line activated by the tamper detection circuit will erase the second volatile memory in the encryption device).

As per claim 10, Rager et al. also describes:

a circuit arrangement providing for erasure of sensitive data, comprising:

a first memory element (see column 2, lines 62-63; figure 1, item 102; a first volatile random access memory (RAM)),

a register (see column 2, lines 66-67; a second volatile memory (RAM)),

a security circuit configured to detect a security threat to the circuit arrangement (see column 4, lines 40-43; figure 1, items 101 and 106; a tamper detection circuit) and

Art Unit: 2132

generate a first signal upon detection of a security threat (see column 4, lines 44-49; figure 1, item 106; activating the reset line to erase memory);

a power supply coupled to the first memory element, the register, and the security circuit (see column 5, lines 65-68; column 6, lines 1-8; figure 1, items 102, 106, and 101; in the event of a power down, the change in power affects the first volatile memory, the second volatile memory and the tamper detection hardware suggesting that all three elements are coupled to the power supply),

the power supply arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source (see column 4, lines 37-40; figure 1, item 101 and 105; a variable power supply powering down the secure transmission device while a constant voltage supply is providing a constant voltage to the encryption device); and

a processor coupled to the first memory element, the register, the security circuit, and the power supply (see column 5, lines 65-68; column 6, lines 1-8; figure 1, items 102, 105, 106, and 101; in the event of a power down, the change in power affects the processor, the first volatile memory, the second volatile memory, and the tamper detection hardware suggesting that all four elements are coupled to the power supply),

the processor configured to store sensitive data in the first memory element when power is available from the first source (see column 4, lines 31-32; figure 1, item 102; prior to power down, the decrypted encryption code is stored in the first volatile memory), and

Art Unit: 2132

upon application of power from the second power source (see column 4, lines 31-40; figure 1, item 101; powering down the secure transmission device; see column 4, lines 37-40; figure 1, item 105; while providing a constant voltage to the encryption device),

copy the sensitive data from the first memory element to the register (see column 4, lines 31-34; figure 1, items 102 and 106; storing the decrypted encryption code and key from the first volatile memory into the second volatile memory), and

erase the sensitive data from the first memory element (see column 4, lines 34-36; figure 1, item 102; erasing the decrypted encryption code and keys stored in the first volatile memory).

As per claim 11, Rager et al. further discusses:

that the processor is further configured to copy the sensitive data from the register to the RAM (see column 6, lines 54-55; figure 3, step 306; storing recaptured encryption code and the recaptured key in the first volatile memory from the second volatile memory in the encryption device) upon reapplication of power from the first source (see column 6, line 15; figure 3, step 300; upon power up),

As per claim 12, Rager et al. also shows:

that the sensitive data includes a general encryption key (see column 4, lines 13-16; figure 1, item 102; the first volatile memory, which may comprise RAM, is used to store the decrypted keys only while the secure transmission device is powered up; see column 4, lines 56-57; storing a key in the first volatile memory).

Allowable Subject Matter

8. Claims 4, 5, 13, and 14 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

9. Claims 7 and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter:

Claims 4 and 5; 7 and 8; and 13 and 14 are drawn to two methods for managing sensitive data, and a circuit arrangement providing for erasure of sensitive data. The closest prior art, Rager et al., U.S. Patent No. 5,363,447 A, in view of Mitsubishi Heavy Ind. Ltd. (Arakawa), Japanese Patent Application Publication No. 08-095866 A, discloses similar methods and circuit arrangement. Rager et al. explains a second memory element that is electrically erasable programmable read-only memory (EEPROM) external to the processor used to store encrypted data (see column 4, lines 8-10; figure 1, item 103; a non-volatile memory which may comprise EEPROM used to store encrypted representations of the encryption code and key(s)). But, Arakawa describes using volatile random access memory RAM instead of non-volatile EEPROM because the information is lost by tampering with the supply of power to this memory (see ¶ [0017]; drawing 1, item 1 and drawing 2, item 11). In spite of this teaching, Rager et al. teach away from having the first memory element internal to the processor to be written to directly by an external keying device (see column 3, lines 12-26; figure 1, items 100 and 102).

Art Unit: 2132

This particular feature explicitly incorporated in intervening claims 4, 7, and 13 renders dependent claims 4 and 5; 7 and 8; and 13 and 14, respectively, to have allowable subject matter.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Blackledge, Jr. et al., U.S. Patent No. 5,341,422 A, describes a secure personal computer capable of deleting sensitive data upon attack
- Grider et al., U.S. Patent No. 5,515,540 A, discloses a microprocessor with power from either a system power supply or battery that wipes out encryption registers upon a security violation
- Charron, U.S. Patent No. 6,732,274 B1, a protection device generating a random number unique to an electronic apparatus

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

Art Unit: 2132

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

June 24, 2005


JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100